UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,	:	19-CR-543 (ARR)
-against-	:	
EZHIL SEZHIAN KAMALDOSS, also known as "Kamaldoss Sezhian," "Kamal Doss" and "Ezhil Cezhian,"	:	**OPINION & ORDER**
and	:	
VELAUDAPILLAI NAVARATNARAJAH, also known as "Rajah,"	:	
Defendants.	:	

ROSS, United States District Judge:

Table of Contents

On April 9, 2021, a grand jury sitting in the Eastern District of New York returned an indictment charging defendants, Ezhil Sezhian Kamaldoss and Velaudapillai Navaratnarajah, with conspiracy to distribute and possess with intent to distribute several Schedule IV controlled substances (Tramadol, Alprazolam, and Carisoprodol) in violation of 21 U.S.C. §§ 846 and 841(b)(2); attempted distribution and possession with intent to distribute one or more of these substances in violation of 21 U.S.C. § 841(b)(2); distribution and possession with intent to distribute the same substances in violation of 21 U.S.C. § 841(b)(2); and conspiracy to launder money in violation of 18 U.S.C. § 1956(h).[1] Superseding Indictment, ECF No. 119. These charges relate to an alleged transnational scheme, the investigation of which began in early 2018 and was carried out by several United States agencies, including the Food and Drug Administration ("FDA") and the Department of Homeland Security, Homeland Security Investigations ("HSI"). *See* Gov't's Mem. Law in Opp'n to Defs.' Mots. to Suppress Evid. 2 ("Gov't Opp'n"), ECF No. 166.

Defendants now move to suppress various pieces of evidence. *See generally* Def. Kamaldoss's Mem. of Law in Supp. of Pre-Trial Mots. ("Kamaldoss Mot."), ECF No. 159; Def. Navaratnarajah's Mem. of Law in Supp. of Pre-Trial Mots. ("Navaratnarajah Mot."), ECF No. 163. Mr. Kamaldoss also moves to dismiss his underlying and superseding indictments on the grounds that the FDA, which led the investigation, lacked statutory authority to pursue this matter. *See* Kamaldoss Mot. 36. For the reasons that follow, defendants' motions are denied in their entirety.

BACKGROUND

In early 2018, the FDA and other agencies began investigating a transnational scheme

[1] Mr. Kamaldoss was first indicted for conspiracy to distribute and possess with intent to distribute Tramadol on November 15, 2019. Indictment, ECF No. 83. This indictment was superseded by the April 9, 2021, indictment charging both Mr. Kamaldoss and Mr. Navaratnarajah with this and other counts. *See* Superseding Indictment, ECF No. 119.

involving shipments of misbranded prescription drugs from distributors abroad to individuals and entities in the United States. Gov't Opp'n 2. Once in the United States, the products—including Tramadol and Alprazolam, a Schedule IV synthetic opioid and a Schedule IV benzodiazepine, respectively—were repackaged by the recipient individuals and entities and mailed to domestic customers. *Id.*

On or about March 21, 2018, Special Agent Patrick Connor, an undercover agent with the FDA, received an unsolicited text message from an individual who later identified himself as "James Wills." Kamaldoss Mot. 2; Gov't Opp'n 2. Mr. Wills said he was from an online pharmacy and offered to sell Agent Connor medications, including 100 milligram pills of Tramadol. Kamaldoss Mot. 2−3; Gov't Opp'n 2−3. Over the course of their text exchanges, Agent Connor ascertained that Mr. Wills was willing to sell thousands of Tramadol pills in bulk shipment. Gov't Opp'n 3. Between March and July 2018, Agent Connor and other law enforcement agents conducted a series of controlled buys from Mr. Wills. *Id.*; Kamaldoss Mot. 3. For example, on or around March 21, 2018, Mr. Wills agreed to sell undercover agents pills of Tramadol and Alprazolam, of which the agents took custody on or about April 16, 2018. Compl. ¶¶ 6–9, ECF No. 2; Gov't Opp'n 3 (noting that Xanax is a brand name of Alprazolam).

In the course of investigating the origin of these drugs, law enforcement agents interviewed two confidential informants in or about July 2018; these informants relayed that Mr. Kamaldoss and Mr. Navaratnarajah owned a company, Hosea Express, that was importing millions of unapproved medications from India through a facility at John F. Kennedy International Airport ("JFK Airport") and mailing the medications to individuals throughout the United States. Kamaldoss Mot. 4; Gov't Opp'n 3. The informants pointed agents to a warehouse in Queens, New York, which they alleged was Hosea Express's base of operations. Kamaldoss Mot. 4; Gov't Opp'n

3. Beginning in July 2018 and continuing through about August 2019, agents surveilled this warehouse, using methods including pole cameras. Gov't Opp'n 3; Navaratnarajah Mot. 3. During their surveillance, agents observed defendants and others on the warehouse's loading ramp. Gov't Opp'n 3. Agents also regularly observed individuals unloading boxes from trucks and loading packages into other vehicles; these packages were then driven to various locations, including a post office in Fresh Meadows, Queens. *Id.* After speaking with employees at the Fresh Meadows post office, agents learned that Mr. Kamaldoss went there almost daily, regularly mailed hundreds of United States Postal Service ("USPS") Priority Mail flat rate envelopes to addresses across the country, and always paid in cash. *Id.* at 3–4. The government later learned that Mr. Navaratnarajah routinely mailed a large number of packages at this post office as well. *Id.*; Navaratnarajah Mot. 3.

On August 29, 2018, Special Agent Connor and a postal inspector observed Mr. Kamaldoss mail eighty-eight packages at the Fresh Meadows post office. Kamaldoss Mot. 5. The postal inspector proceeded to detain five of the packages, which bore the same sender name and return address as those listed on the packages Agent Connor purchased from Mr. Wills: "Andrew Fistel, 124-10 Metropolitan Aenue [*sic*] suite #3." *Id.* Pursuant to a warrant obtained the following day, the packages were searched and revealed to contain Tramadol and Alprazolam. *Id.*; Gov't Opp'n 4.

On January 8, 2019, after observing Mr. Navaratnarajah mail several USPS Priority Mail flat rate envelopes at the Fresh Meadows post office, agents coordinated with postal inspectors to detain four of the mailed packages. Navaratnarajah Mot. 5; Gov't Opp'n 4. The packages—which also bore the name and return address of Andrew Fistel, *see* Gov't Opp'n 34—were brought to the United States Postal Inspection Service in Brooklyn, where they remained until January 23, 2019, when agents obtained a warrant to search them. Navaratnarajah Mot. 5. The packages were also found to contain Tramadol. Gov't Opp'n 4.

During the course of this investigation, Mr. Kamaldoss, a resident and native of India, traveled to the United States on several occasions. Kamaldoss Mot. 6. Mr. Kamaldoss always entered the United States by way of JFK Airport—once on June 7, 2018, again on April 23, 2019, and finally on August 15, 2019. *See id.* 3–4, 6–9, 11–14; Gov't Opp'n 4, 5–7. According to Mr. Kamaldoss, during each of his entries, he was brought by border agents to a secondary inspection area where he was detained and subjected to a search of his electronic devices, Kamaldoss Mot. 3–4, 6–9, 11–14; according to the government, neither Mr. Kamaldoss nor his electronic devices were searched during Mr. Kamaldoss's June 7, 2018, entry into the United States, Gov't Opp'n 5–7.

Of relevance to Mr. Kamaldoss's motions, following the April 23, 2019, border search and based in part on electronic evidence viewed during that search, the government obtained a series of search warrants: one to re-search a copy of the electronic material taken from Mr. Kamaldoss's devices during the April 23 search; one to search materials related to his Apple iCloud account; and two to search email communications associated with Mr. Kamaldoss's two Yahoo email addresses. Kamaldoss Mot. 8−11.

Mr. Kamaldoss was arrested on September 12, 2019. *Id.* at 14. Mr. Navaratnarajah was arrested on February 1, 2020. Navaratnarajah Mot. 5. On April 9, 2021, a grand jury in this district returned a superseding indictment charging both defendants with various counts related to conspiracy and attempt to distribute controlled substances and conspiracy to launder money. Kamaldoss Mot. 14; Navaratnarajah Mot. 5.

Procedural History

On February 14, 2022, and February 27, 2022, Mr. Kamaldoss and Mr. Navartnarajah each moved to suppress evidence in this case and for various other forms of relief. Specifically, Mr. Kamaldoss seeks to suppress the contents of the packages that were seized by agents on August

29, 2018; evidence obtained from his electronic devices during the June 7, 2018, and April 23, 2019, border searches and the fruits thereof;[2] and materials and communications searched in connection with his Apple iCloud account and Yahoo email addresses. *See* Kamaldoss Mot. Mr. Kamaldoss also seeks to dismiss his underlying and superseding indictments. *See id.* at 36. Mr. Navaratnarajah moves to suppress the contents of the packages seized by agents on January 8, 2019, and, pursuant to Federal Rule of Criminal Procedure 12, joins Mr. Kamaldoss's motions to the extent that they apply to him. *See* Navaratnarajah Mot. On March 16, 2022, the government filed its opposition to Mr. Kamaldoss's and Mr. Navaratnarajah's pre-trial motions, *see* Gov't Opp'n, to which both defendants replied on March 30, 2022, *see* Def. Kamaldoss's Reply Mot. ("Kamaldoss Reply"), ECF No. 167; Def. Navaratnarajah's Reply Mot. ("Navaratnarajah Reply"), ECF No. 168.

On April 12, 2022, I held a limited evidentiary hearing on two discrete issues relevant to the motions before me: first, whether a June 7, 2018, border search occurred; and second, whether Mr. Kamaldoss was in custody during the April 23, 2019, border search. Mr. Kamaldoss took the stand and testified as to both matters. In support of its arguments, the government proffered three witnesses: United States Customs and Border Protection ("CBP") Officer Robert Pierce III, who was working in primary inspection at JFK Airport and stamped Mr. Kamaldoss's passport on June 7, 2018; HSI Special Agent Chatchai Chunton, who Mr. Kamaldoss alleges was involved in the

[2] Mr. Kamaldoss additionally requests suppression of evidence obtained during the August 15, 2019, border search. *See* Kamaldoss Mot. 14–30. I need not address this search, however, as the government does not intend to introduce at trial any evidence obtained therefrom. Moreover, the evidence that Mr. Kamaldoss seeks to suppress—such as the contents of his intercepted packages and communications associated with his Apple iCloud and email accounts—did not come from information the government learned during the August 15, 2019, search. Accordingly, I evaluate only the June 7, 2018, and April 23, 2019, border searches in resolving Mr. Kamaldoss's motions.

June 2018 and April 2019 border searches; and CBP Officer Roy Clark, who was assigned to secondary inspection on April 23, 2019, and was involved in seizing Mr. Kamaldoss's electronic devices on that day and inquiring about their passcodes. In addition, the government made Egbert Simon, a supervisory CBP officer, available to defense counsel for cross-examination. Although Officer Simon did not testify on direct examination, I give his affidavit, filed by the government on March 16, 2022, *see* Gov't Opp'n, Ex. A ("Simon Decl."), ECF No. 166-1, the same weight as direct testimony because he was subject to cross-examination. *Cf. United States v. Robles*, 253 F. Supp. 2d 544, 549 n.14 (S.D.N.Y. 2002) ("[C]ourts give greater weight to witness testimony, which was subject to cross examination, than to sworn affidavits." (internal quotation marks, citation, and modifications omitted)).

DISCUSSION

I. The June 7, 2018, Border Search.

On June 7, 2018, Mr. Kamaldoss traveled from India to the United States, arriving at JFK Airport. Kamaldoss Mot. 3−4; Gov't Opp'n 6. Concerningly, while the government contends that its records from that day show only that Mr. Kamaldoss was "uneventfully processed," *see* Gov't Opp'n 6, Mr. Kamaldoss submits that upon arriving at the airport, he was detained and escorted by government agents to a secondary inspection area, where his devices were seized, unlocked, and reviewed by agents for one to two hours, Kamaldoss Mot. 3–4. Based on the cumulative evidence in the record—including the testimony of Mr. Kamaldoss, CBP Officer Pierce, and Special Agent Chunton—I conclude that Mr. Kamaldoss was not subjected to a secondary search on this date.

At the April 12 evidentiary hearing, Mr. Kamaldoss took the stand and testified that on

June 7, 2018, he was taken by an officer at JFK Airport to a secondary inspection room,[3] where he was "told" by two officers to hand over his electronic devices (at the time, Mr. Kamaldoss was carrying two phones and one laptop), as well as all papers and objects in his pockets. Apr. 12 Tr. 19:21−24:15; 28:4−23; 29:19−25 ("Tr."). Mr. Kamaldoss was then asked for and gave the passwords to his devices. *Id.* at 34:3−11. Once handed over, his devices were taken elsewhere, as was Mr. Kamaldoss's luggage. *Id.* at 30:24−31:20. Thereafter, the officers proceeded to question Mr. Kamaldoss for approximately thirty minutes without explaining why Mr. Kamaldoss was in secondary inspection. *Id.* at 32:9−22; 36:8−10. Eventually, Mr. Kamaldoss's belongings were returned to him, and he was allowed to formally enter the United States. *See id.* at 37:3−17; Kamaldoss Mot. 4. Mr. Kamaldoss alleges that, in total, he spent around two hours in secondary inspection. Tr. 32:23−33:4. During this time, he believes that the agents who took his devices unlocked them and reviewed the information therein. Kamaldoss Decl. ¶ 6. Mr. Kamaldoss recalled only that the officers involved in this encounter were wearing uniforms; he was unable to recall what either of them looked like. Tr. 30:4−7.

Following Mr. Kamaldoss's testimony, CBP Officer Pierce and Special Agent Chunton credibly testified that no secondary inspection occurred on June 7. On that day, Officer Pierce—employed by CBP since 2015, *id.* at 127:16−19—was working in primary inspection, through which all travelers are required to pass upon disembarking from their planes, *id.* at 128:1−19; 135:17−18. Mr. Kamaldoss was among the more than 100 passengers whom Officer Pierce processed that day. *Id.* at 136:1−9. According to CBP's TECS System's Person Encounter List ("TECS List") and Officer Pierce's review of the same, Mr. Kamaldoss was not referred to

[3] Although Mr. Kamaldoss did not characterize this room as a "secondary inspection" area, I assume based on his testimony and his counsel's briefs on this motion that this is what he understood it to be. *See* Kamaldoss Mot. 3.

secondary inspection on that date. *See id.* at 136:21−139:24 (explaining that the "ref" column on the TECS List refers to the basis for referring someone from primary to secondary inspection and that the column is blank when someone was not referred); Kamaldoss Mot., Ex. B ("TECS Person Encounter List"), ECF No. 159-1 (showing a blank "ref" column for Mr. Kamaldoss on the date of June 7, 2018). The TECS List is critical evidence in this case: When a traveler is referred from primary to secondary inspection, the referral must be recorded in the TECS List because, *inter alia*, the referral explains to secondary inspection officers the reasons why a traveler is coming to secondary inspection. Tr. 132:8−133:16; 156:2−6. Indeed, officers who fail to record referrals in the TECS system may be subject to disciplinary action. *Id.* at 140:19−25. According to Officer Pierce, in his time working for CBP, he has never failed to record an individual whom he referred to secondary inspection. *Id.* at 133:17−19. In addition to recording referrals in the TECS List, border agents are required to complete an electronic media memorandum any time data is extracted from the electronic devices of a traveler who has been referred to secondary inspection. *Id.* at 133:23−134:17. Officer Pierce testified that, from his review of all records relating to June 7, 2018, no such memorandum exists for Mr. Kamaldoss. *Id.* at 139:23−140:4. Based on the TECS List and the lack of an electronic media memorandum, Officer Pierce stated that it was "highly unlikely" that Mr. Kamaldoss was subjected to a secondary search. *Id.* at 140:13−17.

This conclusion was echoed by Officer Simon, *see* Gov't Opp'n, Ex. A ¶ 8, ECF No. 166-1, as well as Agent Chunton, who was involved in the April 23, 2019, border search of Mr. Kamaldoss, *see* Tr. 167:19−25; 170:19−171:1. In fact, according to Agent Chunton, it wasn't until April 2019 that a "lookout," which alerts border agents to travelers who should be sent to secondary inspection for further processing, was first entered for Mr. Kamaldoss in the CBP system. *Id.* at 131:15−25; 167:4−18. And, critically, in light of his role as case agent in Mr.

Kamaldoss's case, Agent Chunton was unaware of any evidence obtained from Mr. Kamaldoss prior to April 2019. *Id.* at 171:7−10.

While the testimony of Officers Simon and Pierce and Agent Chunton contradicts that of Mr. Kamaldoss, I find the government's witnesses credible and their testimony consistent with each other and with the documentary evidence in this case: the TECS List, which shows that Mr. Kamaldoss was not referred to secondary inspection, and the government's submission that no evidence exists of a June 7 secondary search, *see* Gov't Opp'n 5−7. Mr. Kamaldoss has failed to impugn this fulsome record.[4] In light of this and in the absence of any records corroborating the extraction of data from Mr. Kamaldoss's devices, I find that a secondary inspection did not occur on June 7, 2018, and do not factor such an inspection into my analysis of Mr. Kamaldoss's subsequent claims.

II. The April 23, 2019, Border Search.

On April 23, 2019, Mr. Kamaldoss, his wife, and their two young sons arrived at JFK Airport from India. Kamaldoss Mot. 6. At approximately 4:30 p.m., as the family was proceeding through the airport, a CBP officer directed them to a secondary inspection area. *Id.* There, Special Agent Chunton questioned Mr. Kamaldoss about his plans for his visit to the United States, a previous trip to the country, and his current and past employment. *Id.* at 7. According to Mr. Kamaldoss, Agent Chunton directed Mr. Kamaldoss to open his luggage, which revealed a Dell

[4] Mr. Kamaldoss seems to ask that I infer that the absence of any record pertaining to a June 7 secondary border search of him is explained by human error in failing to record such a search. *See* Tr. 152:16−153:4. I decline to make this inference. No referral to secondary inspection was recorded for Mr. Kamaldoss on this date, unlike on April 23, 2019, and August 15, 2019, when his referrals were recorded, *see* TECS Person Encounter List. Moreover, no CBP or HIS agent had any recollection of a secondary inspection of Mr. Kamaldoss taking place on June 7, 2018. In the face of this abundant evidence, I find Mr. Kamaldoss's argument unpersuasive.

laptop (the "laptop"). *Id.* Eventually, Agent Chunton asked Mr. Kamaldoss for the passwords to his laptop and to his iPhone (the "iPhone" or the "cell phone"). *Id.* After Mr. Kamaldoss supplied his passwords, Agent Chunton turned the devices over to a waiting HSI Computer Forensic Agent. *Id.*

Once in possession of these devices, the HSI Computer Forensic Agent imaged[5] them and, using a forensic software program called Cellebrite,[6] extracted data from Mr. Kamaldoss's iPhone.[7] *Id.*; Kamaldoss Mot., Ex. H, ECF No. 159-1. At approximately 7 p.m., Mr. Kamaldoss's electronic devices were returned to him, and he and his family were permitted to leave the secondary inspection area. Kamaldoss Mot. 8.

Two days later, on April 25, 2019, Special Agent Chunton provided Special Agent Connor of the FDA with copies of the images of Mr. Kamaldoss's electronic devices and the data extracted from Mr. Kamaldoss's iPhone (collectively, the "forensic copies"). Kamaldoss Mot., Ex. G, at 4, ECF No. 159-1. According to Mr. Kamaldoss, Agent Connor searched the images and extracted information at least five times over the next few months: once on May 2, once on May 11, twice on June 14, and once on June 24. *See* Kamaldoss Mot. 8, 28. Though in May 24, 2019, Special Agent Connor applied for and obtained a warrant authorizing his search of the forensic copies, *see* Kamaldoss Mot., Exs. D ("Forensic Search Warrant Appl.") & K ("Forensic Search Warrant"),

---

[5] Imaging refers to the act of "creat[ing] a digital copy of the hard drive that is identical to the original in every relevant respect." Office of Legal Education, Executive Office for United States Attorneys, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 78, https://www.justice.gov/file/442111/download (last accessed Apr. 22, 2021).

[6] According to Mr. Kamaldoss, Cellebrite "enables the extraction and review of specific data sources from an iPhone, including text messages, emails, contacts, and call logs." Kamaldoss Mot. 7 n.6.

[7] Mr. Kamaldoss alleges that in addition to extracting data from his cell phone, the Computer Forensic Agent generated a report detailing the phone's contents. *Id.* at 7–8. Based on my review of the "Cellebrite Extraction Report," submitted by Mr. Kamaldoss as Exhibit H to his Suppression Motion, it appears that the report was in fact generated approximately one month after the extraction. *See* Kamaldoss Mot., Ex. H, ECF No. 159-1 (listing "report creation time" as May 27, 2020).

ECF No. 159-1, his two May searches were not conducted pursuant to a warrant. *See* Kamaldoss Mot. 27–28.

Mr. Kamaldoss moves to suppress evidence taken from his electronic devices during the April 23 border search and the fruits thereof, including the May and June searches. As to the border search, Mr. Kamaldoss argues his statements regarding the passwords to his laptop and iPhone were obtained in violation of his Fifth Amendment rights. *See* Kamaldoss Mot. 15–22. He also claims that the search of his electronic devices exceeded the permissible scope of a border search, violating his rights under the Fourth Amendment. *Id.* at 22–26. Based on these constitutional violations, he concludes that evidence obtained from his electronic devices should be suppressed as fruits of the poisonous tree. *Id.* at 20–26. As to the May searches, Mr. Kamaldoss argues that suppression is required because they were not conducted at the border and occurred more than nine days after the initial search of Mr. Kamaldoss's electronic devices, putting them outside the scope of the border search exception to the warrant requirement. *Id.* at 26. Finally, as to the June searches, Mr. Kamaldoss contends that suppression is required because the electronic devices were searched pursuant to the May 24, 2019, warrant, which was based on evidence tainted by the April 23 border search. *Id.* at 27–28**.** Because I find that the May 24, 2019, warrant did not rely upon tainted evidence, *see infra* Discussion III.B, I find this last argument unavailing**.** I address Mr. Kamaldoss's remaining arguments *seriatim.*

A. Because Mr. Kamaldoss was not in custody on April 23, 2019, Mr. Kamaldoss's Fifth Amendment rights were not violated.

Mr. Kamaldoss contends that evidence taken from his electronic devices during the April 23 border search should be suppressed because it was obtained in violation of his Fifth Amendment rights. Specifically, he argues that agents collected this evidence only because he disclosed the passcodes to his devices during an un-*Mirandized* custodial interrogation. *See* Kamaldoss Mot. 15–22. Because I

find that Mr. Kamaldoss was not in custody on April 23, suppression is unwarranted.

Pursuant to the Fifth Amendment, "[s]tatements made during a custodial interrogation are generally inadmissible unless a suspect has first been advised of his or her rights." *United States v. Faux*, 828 F.3d 130, 134 (2d Cir. 2016) (citing *Miranda v. Arizona*, 384 U.S. 436, 444 (1966)). It is undisputed that Mr. Kamaldoss was not advised of his *Miranda* rights on April 23. *See* Kamaldoss Mot. 15; Gov't Opp'n 8. Whether he had to be, however, depends on whether he was interrogated and in custody on that day. *See Rhode Island v. Innis*, 446 U.S. 291, 300–01 (1980). Because the government argues only that Mr. Kamaldoss was not in custody on April 23, *see* Gov't Opp'n 8−13, I focus my analysis on this factor.

"[C]ustody for *Miranda* purposes is not coterminous with . . . the colloquial understanding of custody." *United States v. FNU LNU*, 653 F.3d 144, 152–53 (2d Cir. 2011) (quotations omitted). Instead, "[t]he test for determining custody . . . asks (1) whether a reasonable person would have thought he was free to leave the police encounter at issue and (2) whether a reasonable person would have understood his freedom of action to have been curtailed to a degree associated with formal arrest." *Faux*, 828 F.3d at 135 (internal quotations and citations omitted); *see also United States v. Belitz*, No. 21-CR-693 (JSR), 2022 WL 205585, at *2 (S.D.N.Y. Jan. 24, 2022) ("The 'free to leave' inquiry is a necessary, but not determinative first step, and the second question remains the ultimate inquiry: 'whether there is a formal arrest or restraint on freedom of movement of the degree associated with a formal arrest.'" (quoting *United States v. Newton*, 369 F.3d 659, 670−71 (2d Cir. 2004))). This inquiry is an objective one: "An individual's subjective belief about his or her status generally does not bear on the custody analysis." *Faux*, 828 F.3d at 135. Factors to be considered include "whether a suspect is or is not told that []he is free to leave; the location and atmosphere of the interrogation; the language and tone used by the police; whether the suspect

is searched, frisked, or patted down; and the length of the interrogation." *Tankleff v. Senkowski*, 135 F.3d 235, 244 (2d Cir. 1998) (citations omitted). At the border—"in which compulsory questioning . . . inheres in the situation and [] in which the traveler has voluntarily submitted to some degree of confinement and restraint," *FNU LNU*, 633 F.3d at 153—the nature of the questions asked is also relevant: a *Miranda* advisal *might* be required where the questions fall outside the scope of what a reasonable traveler would expect at the border. *Id.* at 153−54.

According to Mr. Kamaldoss, who testified to the events of April 23, 2019, he, his wife, and his two children were escorted by officers to a secondary inspection area after arriving at JFK Airport. Tr. 39:5−8; 45:12−14; 47:8−10. At first, they were brought to a main room that had about ten people in it. *Id.* at 45:12−23. Although none of the individuals were handcuffed, the room contained chairs that had handcuffs attached, and many of the people in this room were upset or crying. *Id.* at 45:24−46:5. Mr. Kamaldoss and his wife were told that they were required to give officers their electronic devices, passwords, and any effects that they had on their persons. *Id.* at 50:7−20; 54:1−9. Their belongings were then taken away by officers. *See id*. at 53:4−25. After about thirty or forty minutes—during which time agents asked Mr. Kamaldoss "many questions" about why he was in the United States—Mr. Kamaldoss and his family were taken to a different, smaller room. *Id.* at 55:16−56:17. On the stand, Mr. Kamaldoss described this room as "like a cell," *id.* at 56:13, because it was small, empty, and windowless and because the door to the room was closed, *id.* at 57:1−21. Mr. Kamaldoss also testified that this room contained neither toys nor couches. *Id.* at 113:21−23. In his words, it was "worse" than the main room he had been in earlier. *Id.* at 58:3−4. Mr. Kamaldoss and his family remained in this room for more than an hour. *Id.* at 57:24−25. During their time there, they were not offered food or water, nor were they permitted to use the restroom or leave. *Id.* at 58:13−17; 59:1−3. When asked if he ever left the secondary

inspection room to get an additional bag from baggage claim, Mr. Kamaldoss said no. *Id.* at 115:2−6. Eventually, Mr. Kamaldoss's devices were returned to him, and he and his family were allowed to formally enter the United States. *Id.* at 62:17−63:4. In total, the Kamaldoss family spent at least three hours in secondary inspection. *Id.* at 59:6−16.

While the facts alleged by Mr. Kamaldoss would be concerning if true, I find his version of events incredible based on the testimony given by CBP Officer Roy Clark, the secondary inspection officer who obtained Mr. Kamaldoss's electronic devices and passcodes on April 23, and Special Agent Chunton, who was involved in the devices' digital imaging and extraction. According to Agent Chunton, the secondary inspection room to which Mr. Kamaldoss and his family were first brought is "a big waiting area" that contains twenty to fifty chairs and a counter, behind which the secondary officers sit, not unlike "the DMV." *Id.* at 173:18−174:3. Officer Clark described a sky-blue room containing a water fountain, bathroom, and television, which is often turned on to the news or sports. *Id.* at 218:12−19; 219:5−9. Travelers in the secondary inspection room may sit in any chair they want, *id.* at 221:9−11, and, when their name is called by a secondary inspection officer, they walk themselves up to the counter to answer routine questions, *id.* at 174:12−175:9. Frequently, an agent will *ask* a traveler for their electronic devices and passcodes, as Officer Clark did with Mr. Kamaldoss. *Id.* at 175:10−11; 222:15−25; 225:1−6. Individuals are free to say no. *Id.* at 175:12−15; 223:3−224:5.

According to Agent Chunton, when Mr. Kamaldoss and his family arrived in secondary inspection, they were moved to a smaller, private room—a "family room"—so that they would be more comfortable. *Id.* at 176:9−23. This room, as described by Agent Chunton and Officer Clark, is a far cry from the "cell" testified to by Mr. Kamaldoss: notably, it contains toys for children and a couch. *Id.* at 176:23−177:1; 219:1−4. During the time that Mr. Kamaldoss and his family were in

the family room, they were left to themselves, although Mr. Kamaldoss occasionally checked in with Agent Chunton about the status of his family's stay in secondary inspection. *Id.* at 179:23−180:15.

Agent Chunton testified that at no point during this encounter was Mr. Kamaldoss told that he was under arrest. *Id.* at 178:5−6. Indeed, at one point, Agent Chunton accompanied Mr. Kamaldoss to the luggage carousel so they could find a missing bag of Mr. Kamaldoss's. *Id.* at 178:8−18. After he retrieved his missing bag and before returning to secondary inspection, Mr. Kamaldoss separated entirely from Agent Chunton and used the restroom. *Id.* Agent Chunton testified that he was cordial, respectful, and professional during his interactions with Mr. Kamaldoss. *Id.* at 180:19−21. At the end of their encounter, Agent Chunton even helped the Kamaldoss family with their bags. *Id.* at 180:23−181:3.

Having listened to the accounts of Agent Chunton and Officer Clark, I find their testimony credible and consistent. And considering the many substantial discrepancies between Mr. Kamaldoss's testimony and the testimony given by Agent Chunton and Officer Clark—including details about the private room to which Mr. Kamaldoss and his family were taken and the question of whether Mr. Kamaldoss ever went to baggage claim or the restroom—I find Mr. Kamaldoss's testimony unreliable. Therefore, I accord the testimony of Agent Chunton and Officer Clark greater weight and discount the aspects of Mr. Kamaldoss's testimony that conflict with theirs.

In light of these credibility determinations, I am left with testimonial evidence that does not support a finding that Mr. Kamaldoss was in custody: Mr. Kamaldoss was questioned for between thirty to forty minutes in a room that contained other people; he was then moved to a private room that, despite having a closed door, contained couches and toys; his family was left to themselves while they were in this room; Mr. Kamaldoss was never handcuffed, *id. at* 95:4−5; no weapons were ever drawn, *id.* 76:1−4; nor has evidence been adduced that Mr. Kamaldoss or

members of his family were physically restrained at any point. While Mr. Kamaldoss may have believed that he was not free to leave, *see id.* 27:24−28:3—and indeed, Agent Chunton testified that Mr. Kamaldoss was not permitted to leave secondary inspection, as he had not yet been admitted into the United States, *id.* 200:9−12—just because someone is not free to leave does not mean they are "subjected to restraints comparable to those associated with a formal arrest," *FNU LNU*, 653 F.3d at 153 (internal quotation marks and citation omitted). And courts in this circuit have found environments to be non-custodial where the circumstances present were similar or even more restricting than those here. *See, e.g.*, *FNU LNU*, 653 F.3d at 154−55 (finding that a defendant was not in custody at the airport even though she was interrogated in a private room for ninety minutes and was fingerprinted); *United States v. Broughton*, 983 F. Supp. 2d 224, 230−31 (E.D.N.Y. 2013), *aff'd*, 600 F. App'x 780 (2d Cir. 2015) (concluding that a defendant was not in custody when she was moved to a private search room at the airport, where a suspicious item in her luggage was inspected); *United States v. Hassan*, No. 18-CR-603 (ARR), 2019 WL 5684367, at *3 (E.D.N.Y. Nov. 1, 2019) (concluding a defendant was not in custody when "CBP officers took him [to] a separate room, questioned him about his travels, searched his luggage, copied his paperwork, took his cell phone, and would not allow him to be alone"); *United States v. Wilson*, 100 F. Supp. 3d 268, 279−81 (E.D.N.Y. 2015) (finding an interrogation non-custodial when the defendant was escorted to a private room, questioned, and subjected to a physical pat-down).

Because the "substance of CBP questioning[] can be an important factor in determining whether a person was in custody," *Hassan*, 2019 WL 5684367, at *3, the strongest evidence weighing in favor of a finding that Mr. Kamaldoss was in custody is the fact that he was asked for the passcodes to his electronic devices. As an initial matter, because I find Agent Clark's testimony more credible than Mr. Kamaldoss's, I find that, based on the evidence before me, Mr. Kamaldoss

was *asked* for his laptop, iPhone, and their passcodes in secondary inspection, not told that he must hand them over. *See* Tr. 222:15−25; 225:1−6. To be sure, this is "not necessarily the type of question that a reasonable traveler might expect at the border" because it does not relate to admissibility. *Wilson*, 100 F. Supp. 3d at 280. But I decline to find that this single factor transformed an otherwise non-custodial environment into a custodial one. Agent Clark's question was not so accusatory as to change the very fabric of the encounter. *See United States v. Vallerius*, No. 17-CR-20648 (EGT), 2018 WL 2325729, at *4 (S.D. Fla. May 1, 2018), *report and recommendation adopted*, No. 17-CR-20648 (RNS), 2018 WL 2324059 (S.D. Fla. May 22, 2018) (explaining that a defendant was not in custody merely because an agent asked for his passcodes at the airport); *see also Wilson*, 100 F. Supp. 3d at 280 (finding that although an agent's question was not of the type one would normally expect at the border, the "single question . . . alone [was] not sufficient to transform [the] situation into a custodial one"). Considering the many factors that otherwise indicate a non-custodial environment, "the nature of this question . . . does not tip the scales toward a finding that a reasonable person in [Mr. Kamaldoss's] shoes would have felt restraint to the same degree associated with formal arrest." *Wilson*, 100 F. Supp. 3d at 280.

In sum, evaluating the totality of circumstances, I find that Mr. Kamaldoss was not in custody on April 23, 2019, and thus *Miranda* warnings were not required.[8] I turn now to his argument that the events of this day violated his rights under the Fourth Amendment.

B. The April 23, 2019, border search did not violate Mr. Kamaldoss's Fourth Amendment rights.

Mr. Kamaldoss's principal Fourth Amendment argument is that the April 23, 2019, search

[8] I find Mr. Kamaldoss's heavy reliance on *United States v. Djibo*, 151 F. Supp. 3d 297 (E.D.N.Y. 2015), which is not controlling authority, misplaced. While the court in that case concluded that the defendant was in custody, the fact that the defendant was an *outbound*—not inbound— traveler at the time he was stopped by border agents was integral to the court's determination. *Id.* at 306. Here, Mr. Kamaldoss was inbound when he was stopped.

of his electronic devices exceeded the scope of a permissible border search. Kamaldoss Mot. 23–26. Mr. Kamaldoss argues that law enforcement was required to have reasonable suspicion that his electronic devices contained *actual* contraband—not just *evidence* of contraband—when the agents searched them on April 23. *Id.* The government disagrees, contending that law enforcement needed at most reasonable suspicion that Mr. Kamaldoss was committing border-related crimes, which they had here. Gov't Opp'n 23–25. As explained below, I need not decide the level of suspicion that was required to search Mr. Kamaldoss's electronic devices: if reasonable suspicion of a border-related offense was necessary, that standard was clearly met, and under the good faith exception, the search was permissible even if more was required.

1. *Searches of electronic devices at the border.*

The "touchstone of the Fourth Amendment is reasonableness," which is evaluated "by assessing, on the one hand, the degree to which [a search] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *United States v. Knights*, 534 U.S. 112, 118−19 (2001) (internal quotation marks and citation omitted). In considering this inquiry, the Supreme Court has stated that "where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, reasonableness generally requires the obtaining of a judicial warrant." *Riley v. California*, 573 U.S. 373, 382 (2014) (internal quotation marks, citation, and alterations omitted). "In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." *Id.*

Searches at the international border, where "the [g]overnment's interest in preventing the entry of unwanted persons and effects is at its zenith," *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004), have long been held exempt from the warrant requirement. *Id.* at 152–53. This

exception derives from "the longstanding right of the sovereign to protect itself," as well as its authority to collect duties from those entering the country. *Id.* (internal quotation marks and citation omitted). "Routine searches of the persons and effects of entrants are [thus] not subject to any requirement of reasonable suspicion, probable cause, or warrant." *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). Rather, routine "searches made at the border . . . are reasonable simply by virtue of the fact that they occur at the border," *United States v. Ramsey*, 431 U.S. 606, 616 (1977), or its functional equivalent, *see Almeida-Sanchez v. United States*, 413 U.S. 266, 272–73 (1973) (noting that routine border searches "may in certain circumstances take place not only at the border itself, but at its functional equivalents as well"); *United States v. Levy*, 803 F.3d 120, 122 (2d Cir. 2015) ("It is well established that the Customs area of an international airport is the functional equivalent of a border for purposes of the border search doctrine.").

Although this exception is broad, it is not unfettered. While the Supreme Court has not spoken to the precise circumstances under which some level of suspicion is required for a border search, it has suggested that "in the case of highly intrusive searches" where salient "dignity and privacy interests" are at stake, "a requirement of . . . suspicion" might be supported. *Flores-Montano*, 541 U.S. at 152; *see also United States v. Kolsuz*, 890 F.3d 133, 138 (4th Cir. 2018), *as amended* (May 18, 2018) (noting that the Supreme Court has suggested that some level of suspicion might be appropriate for "destructive searches of property and searches carried out in 'particularly offensive' manners" (quoting *Flores-Montano*, 541 U.S. at 152, 154 & n.2)); *Montoya de Hernandez*, 473 U.S. at 541−42 (holding that the detention of a traveler beyond the scope of a routine search required reasonable suspicion that the traveler was smuggling drugs in their alimentary canal). The Second Circuit and several other circuits have since recognized that more invasive searches, such as strip searches, are nonroutine, thus requiring reasonable suspicion. *See*

United States v. Irving, 452 F.3d 110, 123 (2d Cir. 2006); *Kolsuz*, 890 F.3d at 144–47; *United States v. Gonzalez-Rincon*, 36 F.3d 859, 864 (9th Cir. 1994); *United States v. Yakubu*, 936 F.2d 936, 939 (7th Cir. 1991); *United States v. Oyekan*, 786 F.2d 832, 837–39 (8th Cir. 1986). Whether a search is so intrusive that it crosses into the territory of nonroutine hinges on how "deeply [the search] intrudes into a person's privacy." *Kolsuz*, 890 F.3d at 144; *see also Irving*, 452 F.3d at 123 (noting that nonroutine searches are those that "substantially infringe on a traveler's privacy rights").

In the context of searches of electronic devices, this distinction between routine and nonroutine searches is an area of evolving jurisprudence. Faced with the proliferation and ubiquity of electronic devices—without which it is neither "realistic nor reasonable to expect the average [person]" to travel, *United States v. Saboonchi*, 990 F. Supp. 2d 536, 556 (D. Md. 2014)—courts have had to reckon with the conditions under which a search of electronic devices becomes nonroutine and what the Fourth Amendment requires when it does. Neither the Supreme Court nor the Second Circuit has "addressed the issue of border searches of electronic devices." *Abidor v. Napolitano*, 990 F. Supp. 2d 260, 281 (E.D.N.Y. 2013); *see also Irving*, 452 F.3d at 123–24 (declining to determine whether searches of diskettes and film found in a traveler's bag were routine or nonroutine because the searches were supported by reasonable suspicion either way). Of the circuits that have addressed the issue, the Fourth and Ninth Circuits stand alone in concluding that forensic searches of electronic devices, which "generally entail[] the connection of external equipment and/or the use of specialized software," *United States v. Aigebekaen*, 943 F.3d 713, 718 n.2 (4th Cir. 2019), are nonroutine and thus require reasonable suspicion.[9] *See id.*

[9] Unlike manual searches of electronic devices, which do not entail the use of specialized software or connection of external equipment, forensic searches are "'a powerful tool' capable of not only revealing data that a user has intentionally saved on an electronic device, but also 'unlocking password-protected files, restoring deleted material, and retrieving images viewed on websites.'" *Aigebekaen*, 943 F.3d 713, 718 n.2 (4th Cir. 2019) (quoting *United States v. Cotterman*, 709 F.3d

at 720 ("If the border exception applies to the . . . forensic searches of [the defendant's] devices, these searches . . . were sufficiently intrusive to be 'nonroutine' and so required some level of individualized suspicion."); *United States v. Cano*, 934 F.3d 1002, 1016 (9th Cir. 2019) ("[W]e hold that manual searches of cell phones at the border are reasonable without individualized suspicion, whereas the forensic examination of a cell phone requires a showing of reasonable suspicion."); *Kolsuz*, 890 F.3d at 144 (agreeing with the district court that "a forensic border search of a phone must be treated as nonroutine"); *United States v. Cotterman*, 709 F.3d 952, 962 (9th Cir. 2013) ("It is the comprehensive and intrusive nature of a forensic examination . . . that is the key factor triggering the requirement of reasonable suspicion here."). *But see United States v. Touset*, 890 F.3d 1227, 1233 (11th Cir. 2018) ("We see no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property.").

In reaching this conclusion, the Fourth and Ninth Circuits emphasized "the breadth of private information" that can be uncovered from a forensic search, signifying a deep intrusion into a traveler's privacy. *Kolsuz*, 890 F.3d at 144–45; *see Cotterman*, 709 F.3d at 964. Indeed, as the Ninth Circuit explained in *United States v. Cotterman*, 709 F.3d 952, whereas "[t]he amount of private information carried by international travelers was traditionally circumscribed by the size

952, 957 (9th Cir. 2013)). Indeed, CBP appears to distinguish between manual and forensic searches, although it uses different nomenclature. Under CBP policy, advanced searches, which are searches where "an officer connects external equipment [] through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents," should be performed only where "there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern." *See* U.S. Customs and Border Protection, CBP Directive No. 3340-049A, at 5.1.4 (2018), https://www.dhs.gov/sites/default/files/publications/CBP%20Directive%203340-049A_Border-Search-of-Electronic-Media.pdf (last accessed Apr. 21, 2022). A basic search, which is defined as anything other than an advanced search, does not require such suspicion. *Id.* at 5.1.3.

of the traveler's luggage or automobile," such is no longer the case in the digital age. *Id.* at 964. "The average 400-gigabyte laptop hard drive can store over 200 million pages−the equivalent of five floors of a typical academic library." *Id.* (citing Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 542 (2005)). "Laptop computers, iPads and the like are [thus] simultaneously offices and personal diaries. They contain the most intimate details of [a traveler's life]: financial records, confidential business documents, medical records and private emails." *Id.*[10]

In light of the "unparalleled breadth of private information" that can be revealed by a comprehensive forensic analysis, *Kolsuz*, 890 F.3d at 145, there seems to be good reason to consider forensic searches nonroutine and thus demanding of reasonable suspicion. But if they are, this raises another question of first impression in this circuit: "[O]f *what* must the [g]overnment have [reasonable] suspicion for the border search exception to apply?" *Aigbekaen*, 943 F.3d at 720. Put differently, if reasonable suspicion was in fact required to search Mr. Kamaldoss's electronic devices on April 23, was it reasonable suspicion of general criminal activity or something more? While Mr. Kamaldoss and the government seem to agree that the imaging of Mr. Kamaldoss's devices and the use of Cellebrite on his iPhone amounted to a forensic search, *see* Kamaldoss Mot. 25; *see generally*

[10] Integral to the Fourth Circuit's conclusion was the Supreme Court's holding in *Riley v. California*, 573 U.S. 373 (2014), that the search-incident-to-arrest exception to the warrant requirement does not apply to searches of cell phones. *See id.* at 386. The justifications underlying *Riley*, the Fourth Circuit explained, apply with similar force to searches of cell phones at the border: the "immense storage capacity"; "the special sensitivity of the kinds of information that may be stored"; and finally, the pervasive nature of cell phones. *Kolsuz*, 890 F.3d at 145–46 (internal quotation marks and citations omitted). In the Fourth Circuit's view, "*Riley* insists [that] cell phones are fundamentally different 'in both a quantitative and a qualitative sense' from other objects traditionally subject to government searches." *Id.* at 145 (quoting *Riley*, 573 U.S. at 393). Although the holding in *United States v. Kolsuz*, 890 F. 3d 133, was confined to the forensic search of a cell phone at the border, the Fourth Circuit later applied the same reasoning to hold that reasonable suspicion is required to forensically search laptops and iPods at the border. *Aigbekaen*, 943 F. 3d at 721.

Gov't Opp'n 17–25, they disagree on the answer to this question. Mr. Kamaldoss urges me to answer it in accord with the Ninth Circuit, which recently held that border officials may conduct a forensic search of a cell phone only when they reasonably suspect that the cell phone *itself* contains digital contraband, not just evidence of contraband, *Cano*, 934 F.3d at 1020. Kamaldoss Mot. 23−26. The government contends that this distinction between a search for digital contraband and a search for evidence of contraband is misguided because it goes against the purposes of the border-search doctrine and the weight of authority. Gov't Opp'n 22. The government argues that, at most, the forensic search must have been supported by general reasonable suspicion, which was satisfied on April 23 because Agent Chunton had reasonable suspicion that Mr. Kamaldoss was engaged in an international drug trafficking conspiracy. *Id.* at 23–25.

While the Second Circuit has not spoken to the scope of a forensic search at the border, "[a]s a general rule, the scope of a warrant exception should be defined by its justifications." *Kolsuz*, 890 F.3d at 143; *see also Arizona v. Gant*, 556 U.S. 332, 351 (2009) ("When the[] justifications" undergirding an exception to the warrant requirement "are absent, a search . . . will be unreasonable unless police obtain a warrant or show that another exception to the warrant requirement applies."). For this very reason, the Supreme Court has found that the search-incident-to-arrest exception does not apply to warrantless searches of cell phones, where the reasons behind the exception are not present. *See Riley*, 573 U.S. at 386 (concluding that the concerns of officer safety and destruction of evidence are not implicated by digital data stored on a cell phone). Similarly, while "an[] emergency threatening life or limb" may provide a basis for a warrantless search, this exception cannot continue to justify a search once the initial exigency ends. *See Mincey v. Arizona*, 437 U.S. 385, 393 (1978) (holding that a warrantless search based on an exigency must be "strictly circumscribed by the exigencies which justif[ied] its initiation" (internal quotation

marks and citation omitted)). Heeding this precedent and across two cases, the Fourth Circuit has articulated a similar "nexus" requirement for warrantless searches at the border. Concluding that "a direct link between the predicate for the search [at a border] and the rationale for the border exception," existed in *United States v. Kolsuz*, 890 F. 3d 133, *id.* at 143, the Fourth Circuit clarified in *United States v. Aigbekaen*, 943 F.3d 713, that "to conduct [a forensic search] under the border search exception . . . the [g]overnment must have individualized suspicion of an offense that bears some nexus to the border search exception's [historic] purposes of protecting national security, collecting duties, blocking the entry of unwanted persons, or disrupting efforts to export or import contraband," *Aigbekaen*, 943 F.3d at 721. Accordingly, a warrantless forensic search may not be justified by the government's "generalized interest in law enforcement and combatting crime." *Aigbekaen*, 943 F.3d at 721 (internal quotation marks and citation omitted). Under this framework, evidence that a traveler has committed *domestic* crimes, for example, would not provide reasonable suspicion to search an electronic device because domestic offenses are untethered from the historic rationales of the border search exception. *See id*. at 721–22.

While I find this nexus requirement compelling and in line with the lineage of cases articulating the boundaries of exceptions to the warrant requirement,[11] I ultimately need not decide whether this standard is correct as a matter of law. Assuming *arguendo* that it is, it was clearly met during the April 23 border search. "A reasonable suspicion inquiry simply considers, after taking into account all the facts of a particular case, whether [a] border official had a reasonable basis on which to conduct the search." *Irving*, 452 F.3d at 124 (internal quotation marks, alteration, and citation omitted). Under the Fourth Circuit's nexus requirement, the reasonable suspicion must be

[11] At least one other court in this district has expressed that a "showing of reasonable suspicion should be required" if "suspicionless forensic computer searches at the border threaten to become the norm." *Abidor v. Napolitano*, 990 F. Supp. 2d 260, 282 (E.D.N.Y. 2013).

of an offense related to one of the border search exception's justifications. Factors relevant to a court's determination include "unusual conduct of the defendant, discovery of incriminating matter during routine searches, computerized information showing propensity to commit relevant crimes, or a suspicious itinerary." *Id.* By the time Mr. Kamaldoss was stopped at the border on April 23, 2019, border agents had a reasonable basis to believe that he was involved in a transnational conspiracy: the government's investigation of this conspiracy had been ongoing for more than a year and included several controlled buys of Tramadol and Alprazolam; as of July 2018, approximately eight months before the border search, Mr. Kamaldoss had been identified by two confidential informants as a conspirator in the larger importation and distribution scheme; Mr. Kamaldoss had been seen at the very warehouse identified by the informants as the base of operations for the conspiracy; and packages mailed by Mr. Kamaldoss and seized by the government contained Tramadol and Alprazolam. Gov't Opp'n 3−4. Taken together, this information more than supplied border agents with a reasonable basis for believing that Mr. Kamaldoss was engaged in efforts to illegally import scheduled drugs from abroad, an offense directly tied to at least one of the historic rationales for the border exception—the disruption of efforts to import contraband.

Apparently rejecting the Fourth Circuit's approach, Mr. Kamaldoss asks that I instead take the considerable step of adopting the standard for forensic searches articulated by the Ninth Circuit in *United States v. Cano*, 934 F.3d 1002. Noting that "[t]he detection of . . . contraband [itself] is the strongest historic rationale for the border-search exception," the *Cano* court held that border searches are restricted in scope to searches for contraband, and, as a corollary, that forensic searches at the border require reasonable suspicion that the device itself contains contraband.

Cano, 934 F.3d at 1018, 1019–20 (internal quotation marks and citation omitted).[12] Since *Cano*, no other circuit has held that forensic searches of electronic devices should be limited to searches for digital contraband. Indeed, just last year, the First Circuit in *Alasaad v. Mayorkas*, 988 F.3d 8 (1st Cir. 2021), rejected the distinction between searches for contraband and searches for evidence of contraband, holding that the "search[] for evidence is vital to achiev[e] the border search exception's purposes of controlling 'who and what may enter the country.'" *Id.* at 20 (quoting *United States v. Ramsey*, 431 U.S. 606, 620 (1977)).

That said, there may be reasons to limit the scope of forensic searches to digital contraband given the trove of private information contained in electronic devices. *Cf. United States v. Vergara*, 884 F.3d 1309, 1317 (11th Cir. 2018) (Pryor, J., dissenting) ("[F]orensically searching a cell phone may lead to the discovery of physical contraband. . . . But this general law enforcement justification is quite far removed from the purpose originally underlying the border search exception."). But the time for such a decision is not now. In the face of conflicting circuit precedent and the absence of any guidance from the Second Circuit on searches of digital devices at the border, I leave this matter for a later date and a higher court.

Additionally, for the present purposes, I need not determine whether to follow the approach offered in *Cano*: under the good-faith doctrine, exclusion of evidence would be improper even were I to apply that approach in this case. While the "evidentiary fruits of Fourth Amendment violations are generally inadmissible at trial[,] . . . the fruits of 'a search conducted in reasonable reliance on binding [appellate] precedent are not subject to the exclusionary rule,' as that rule is designed 'to deter *future* Fourth Amendment violations,'" *Aigbekaen*, 943 F.3d at 725

[12] Although *Cano* concerned the forensic search of a cell phone, the court noted that there is "no basis to distinguish a forensic cell phone search from a forensic laptop search." 934 F.3d at 1015.

(modification omitted) (quoting *Davis v. United States*, 564 U.S. 229, 236–37, 241 (2011)); *see also Davis*, 564 U.S. at 249–50 ("[W]hen the police conduct a search in objectively reasonable reliance on binding appellate precedent, the exclusionary rule does not apply."). In looking to appellate precedent, I am bound by "the precedent of this [c]ircuit and the Supreme Court." *United States v. Aguiar*, 737 F.3d 251, 261 (2d Cir. 2013). At the time of the April 23, 2019, border search, there was neither Supreme Court nor Second Circuit precedent limiting warrantless forensic searches to digital contraband.[13] In fact, neither court had ever addressed the issue of border searches of electronic devices. Instead, caselaw existed from both courts making clear that, in the context of border searches in general, at most reasonable suspicion was required for some more intrusive searches. *See Flores-Montano*, 541 U.S. at 152; *Irving*, 452 F.3d at 123. Based on the governing law in this circuit, then, the border agents who searched Mr. Kamaldoss's devices had no reason to think that they could do so only if they had reasonable suspicion that the devices contained digital contraband. *Cf. Kolsuz*, 890 F.3d at 148 (declining to decide whether more than reasonable suspicion is required for a forensic border search because either way, agents acted in accordance with applicable law at the time). Because the border agents acted in reasonable reliance on then-existing case law, the digital evidence from Mr. Kamaldoss's devices would not be subject to suppression regardless of whether I apply the *Cano* standard.

2. The May 2, 2019, and May 11, 2019, searches of forensic copies of Mr. Kamaldoss's electronic devices.

On April 25, 2019, Special Agent Chunton provided Special Agent Connor of the FDA with forensic copies prepared from the searches completed on Mr. Kamaldoss's laptop and iPhone.

[13] Indeed, even *Cano*, which is not binding precedent in this circuit, had not been decided as of the April 23, 2019, border search. *See* 943 F.3d at 1019–20. The decision was handed down approximately four months later.

See Kamaldoss Mot., Ex. G, at 4, ECF No. 159-1. According to a "Report of Investigation" prepared by Special Agent Connor, he reviewed these forensic copies on two later dates—May 2, 2019, and May 11, 2019—and neither search was conducted pursuant to a warrant. *See* Kamaldoss Mot., Ex. I, at 2−3, ECF No. 159-1. Mr. Kamaldoss moves to suppress the fruits of these searches, submitting that because the searches were conducted "(a) away from the border, (b) weeks after the data was seized, (c) by, most importantly, a government agent with no authority to conduct border searches," they cannot fall within the border search exception to the warrant requirement.[14] Kamaldoss Reply 12−14; *see also* Kamaldoss Mot. 26−27. The government maintains that Agent Connor's review of the forensic copies on later dates was a continuation of the border search and that such subsequent review is "inherent to any forensic search." Gov't Opp'n 22.

Though I appreciate the parties' arguments, the caselaw on what constitutes a permissible continuation of a border search often involves circumstances quite different from those present here. While other courts have held that "an off-site forensic search of an electronic device over a long period of time is nonetheless a border search," in those cases "the electronic device was seized at the border, the device was never cleared to pass through the border, and therefore the defendant never regained an expectation of privacy in the electronic device." *United States v. Kolsuz*, 185 F. Supp. 3d 843, 851–52 (E.D. Va. 2016) (citation, quotation marks, and modifications omitted), *aff'd*, 890 F.3d 133, *as amended* (May 18, 2018); *cf. United States v. Stewart*, 729 F.3d 517, 526 (6th Cir. 2013) (noting that a defendant had not regained an expectation of privacy in his computers when they were searched before being cleared for entry). In contrast, Mr. Kamaldoss's electronic

[14] In the alternative, Mr. Kamaldoss argues that even if I decide that the searches fall into the border search exception, their fruits should still be suppressed because the searches exceeded the permissible scope of a border search of an electronic device. As discussed above, suppression is not justified under this argument. *See supra* Discussion II.B.1.

devices were returned to him on April 23, 2019, and he was ultimately cleared for entry into the United States. Kamaldoss Mot. 8; Tr. 62:15−63:4. Mr. Kamaldoss thus regained some expectation of privacy in his devices on this date. *See Kolsuz*, 185 F. Supp. 3d at 851–52. That he did, however, does not mean that these later May searches of data taken from his devices were impermissible.

As explained above, *see supra* Discussion II.B.1, the "touchstone of the Fourth Amendment is reasonableness." *Knights*, 534 U.S. at 118. While law enforcement officers are typically permitted to re-search materials already in their possession, in the context of forensic copies created pursuant to a search warrant, the Second Circuit has gestured at the possibility that the long-term retention of such copies may be unreasonable when they contain data that is not responsive to the items called for by the terms of the warrant. In *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016) (en banc), law enforcement agents made forensic images of the hard drives of a company pursuant to a valid search warrant. *Id.* at 200−01. Though agents apparently promised to purge or delete nonresponsive files from their copies, this was never done. *Id.* at 203 n.7. Nearly three years later, when Stavros Ganias, who owned the company whose hard drives had been searched, became a suspect in a separate criminal case, the government obtained a second warrant to search the forensic copies that were seized in relation to the government's earlier investigation. *Id.* at 201, 207. In filing a motion to suppress the fruits of that latter search, Mr. Ganias alleged that the long-term retention of nonresponsive files violated his Fourth Amendment rights. *Id.* at 207–08. While the Second Circuit declined to address the merits of his argument—resolving his claim on good-faith grounds instead, *id.* at 225—it took note of the "privacy concerns implicated when a hard drive or forensic mirror is retained, even pursuant to a warrant," given the "significance of the data kept by many individuals on their [electronic devices]," *id.* at 217−18. Indeed, "[t]he seizure of a computer hard drive, and its subsequent retention by the government,

can give the government possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be *entirely irrelevant* to the criminal investigation that led to the seizure." *Id.* at 217 (emphasis added).

While these concerns "highlight the importance of careful consideration of the technological contours of digital search and seizure," *id.* at 209, I do not find that they warrant suppression in this case. It is likely that the forensic copies searched by Agent Connor on May 2 and May 11 contained data both responsive and nonresponsive to the investigation of Mr. Kamaldoss. *See* Forensic Search Warrant Appl. Nevertheless, these searches occurred within weeks of the initial seizure, and they related to the same and ongoing investigation into a transnational criminal scheme. They did not occur, as was the case in *Ganias*, more than two years after the fact and in the scope of a new investigation. While searches justified at their inception may be rendered unreasonable when circumstances change, *see, e.g.*, *United States v. Place*, 462 U.S. 696, 707−10 (1983) (holding that while the initial seizure of luggage for purposes of subjecting it to a dog-sniffing test was reasonable, the seizure became unreasonable when the seizure was prolonged for ninety minutes); *United States v. Jacobsen*, 466 U.S. 109, 124 (1984) ("[A] seizure lawful at its inception can nevertheless violate the Fourth Amendment because its manner of execution unreasonably infringes possessory interests protected by the Fourth Amendment's prohibition on 'unreasonable seizures.'"), in light of the proximity and relatedness of the May searches to the April 23 border search, I decline to find the May searches unreasonable.

Moreover, suppression of the May searches is barred under the independent source doctrine, which "permits the admission of evidence seized pursuant to an unlawful search if that evidence would have been obtained through separate, lawful means," *United States v. Vilar*, 729 F.3d 62, 83 n.19 (2d Cir. 2013) (citing *Murray v. United States*, 487 U.S. 533, 537 (1988)). "Where

evidence is obtained pursuant to a warrant issued after an illegal search, the independent source doctrine applies if[] '(1) the warrant was supported by probable cause derived from sources independent of the illegal search; and (2) the decision to seek the warrant was not prompted by information gleaned from the illegal conduct.'" *United States v. Mulholland*, 702 F. App'x 7, 10 (2d Cir. 2017) (summary order) (quoting *United States v. Johnson*, 994 F.2d 980, 987 (2d Cir. 1993)). Assuming for argument's sake that the May 2 and May 11 searches were illegal, their fruits would still be admissible under this doctrine. In June 2019, Special Agent Connor reviewed the same forensic copies pursuant to a May 24, 2019, search warrant. As described below, *see infra* Discussion III.B, the May 24 warrant was supported by probable cause derived from the April 23 border search—a source independent from the May 2 and May 11 searches. "That the second element is satisfied is evident from the warrant application[] [itself]," *United States v. Loera*, 333 F. Supp. 3d 172, 187 (E.D.N.Y. 2018), which makes no reference to the May searches, *see* Forensic Search Warrant Appl. ¶¶ 24−57. Instead, the warrant application's grounds for probable cause are evidence adduced from months of investigation and information gleaned from the April 23 border search—not the subsequent searches of forensic copies created on that day. *See id.*; *see also infra* n.17 (concluding that paragraphs fifty-one through fifty-three of the search warrant application are based on information learned during the border search).

In light of the foregoing, I find the contents of the May 2, 2019, and May 11, 2019, border searches admissible. I now turn to Mr. Kamaldoss's and Mr. Navaratnarajah's remaining motions, which largely concern the admissibility of material searched pursuant to warrants.

III. Materials Searched Pursuant to a Warrant.

A. The August 29, 2018, and January 8, 2019, intercepted packages.

As detailed above, on August 29, 2019, and January 8, 2019, postal inspectors seized sets

of packages mailed by Mr. Kamaldoss and Mr. Navaratnarajah, respectively. While agents obtained a warrant to search the packages dropped off by Mr. Kamaldoss within one day of the packages' seizure, Kamaldoss Mot. 5, they did not procure a warrant to search the packages mailed by Mr. Navaratnarajah until fifteen days after the agents seized them, Navaratnarajah Mot. 4. Once searched, both sets of packages were revealed to contain Tramadol. Gov't Opp'n 4 (noting that the packages dropped off by co-defendants contained Tramadol and that the packages mailed by Mr. Kamaldoss also contained Alprazolam). Mr. Kamaldoss and Mr. Navaratnarajah now independently move to suppress the contents of these packages, contending that the government's delays in obtaining search warrants were constitutionally unreasonable.[15] *See* Kamaldoss Mot. 30−31; Navaratnarajah Mot. 5−10. Considering the balance of factors, I find that the delays in obtaining search warrants to search the packages were not unreasonable.

"It has long been held that first-class mail such as letters and sealed packages subject to letter postage . . . is free from inspection by postal authorities, except in the manner provided by the Fourth Amendment." *United States v. Van Leeuwen*, 397 U.S. 249, 251 (1970). This does not mean, however, that absent a warrant, "first-class mail is [] beyond the reach of all inspection." *Id.* at 252. A package may be temporarily detained without a warrant for purposes of investigation, "provided [that] (1) law enforcement authorities have a reasonable suspicion of criminal activity; and (2) the packages are not detained for an unreasonable length of time" before a search warrant is secured. *United States v. Martinez*, 869 F. Supp. 202, 205 (S.D.N.Y. 1994). Regarding this

[15] Mr. Kamaldoss alternatively argues that suppression is appropriate because, in obtaining a warrant to search the packages, the government relied on information learned during its June 7, 2018, border search. Kamaldoss Mot. 34. As an initial matter, the application in support of a warrant to search Mr. Kamaldoss's packages makes no mention of a June 7, 2018, border search. *See generally* Kamaldoss Mot., Ex. A, ECF No. 159-1. Moreover, as discussed above, *see supra* Discussion I, I have already found that no forensic search took place on June 7, 2018. This argument is thus without merit.

second prong, the Second Circuit has articulated four factors that are "generally relevant to whether the police have waited an unreasonable amount of time before seeking a search warrant": (1) the length of the delay; (2) the importance of the seized property to the defendant; (3) whether the defendant had a reduced property interest in the seized item; and (4) the strength of the state's justification for the delay. *United States v. Smith*, 967 F.3d 198, 206 (2d Cir. 2020).

Factors two and three, which look the same across both co-defendants here, strongly weigh toward finding that law enforcement agents' one- and fifteen-day delays in securing search warrants were reasonable. As to the second factor—the importance of the seized property to the defendant—although Mr. Kamaldoss and Mr. Navaratnarajah both had a Fourth Amendment interest in their packages, *see United States v. Martin*, 157 F.3d 46, 54 (2d Cir. 1998), the packages were not personal effects. Indeed, the packages were misbranded drugs imported from abroad that were being distributed to domestic third parties. To the extent that the seized packages were important to Mr. Kamaldoss and Mr. Navaratnarajah, their importance was minimal at best. *Cf. Smith*, 967 F.3d at 207 (finding that the seized property—a personal tablet computer, which contained "immense amounts of personal data," much of which had "nothing to do with the investigation of criminal activity"—was important to the defendant). As to the third factor, both Mr. Kamaldoss's and Mr. Navaratnarajah's possessory interests in their packages were substantially diminished. An individual's possessory interest in their property is already reduced when that property is put into the stream of mail. *See United States v. Okparaeke*, No. 17-CR-225 (NSR), 2018 WL 4003021, at *12 (S.D.N.Y. Aug. 21, 2018) ("Defendant's possessory interest was diminished by sending the package through United Parcel Service."); *Martin*, 157 F.3d at 54 (noting that a seizure is less intrusive where the owner has relinquished control of the property to USPS); *see also Smith*, 967 F.3d at 208 & n.2 (collecting cases where courts have found a

diminished property interest "because the property had been . . . voluntarily relinquished to a third party"). Here, however, the packages not only were relinquished to USPS but also all bore the same fictitious name and return address: "Andrew Fistel, 124-10 Metropolitan Aenue [*sic*] suite #3." Gov't Mot. 34. Based on this, there is strong reason to believe that it would have been difficult, if not impossible, for Mr. Kamaldoss and Mr. Navaratnarajah to retrieve their packages if they had so desired. *Cf. United States v. Pitts*, 322 F.3d 449, 456−57 (7th Cir. 2003) (explaining that because a co-defendant who used a false return address had no legitimate way of retrieving it, the package was therefore abandoned). Considering these facts, I find that their possessory interests in the packages were substantially reduced.

Factor four—the strength of the state's justification for the delay—weighs in favor of Mr. Navaratnarajah. In advance of the April 12 evidentiary hearing, the government proffered that (1) as of the date that Mr. Navaratnarajah's packages were seized—January 8, 2019—the government had all the information necessary to obtain its search warrant, and (2) the affiant who secured the search warrant could not recall any particular reason why the warrant was not secured until fifteen days after their seizure. Letter in Opp'n 4, ECF No. 174. Accordingly, there is no basis for finding that the government was justified in its delay.

As for the fourth factor's application to Mr. Kamaldoss, at the time of the August 29 seizure, the government's investigation into Mr. Kamaldoss had been ongoing for several months and it had gathered credible evidence that he was involved in a drug distribution conspiracy. *See supra* Background (explaining that, by August 29, 2018, Mr. Kamaldoss had been identified by two confidential informants and observed at the warehouse identified as the base of operations). It therefore appears that the government was in possession of sufficient information to obtain a warrant to search the packages on August 29. It did not obtain a warrant, however, until a day later.

Even with a mere one-day delay between the seizure and the warrant, therefore, this factor may weigh in Mr. Kamaldoss's favor, albeit only very slightly.

Turning finally to the first factor, the length of the delay, I find that this factor also weighs differently across co-defendants. Turning first to Mr. Kamaldoss, the one-day delay between when his packages were seized and when a warrant was obtained to search them was not material. In *United States v. Van Leeuwen*, 397 U.S. 249, the Supreme Court explained that "[n]o interest protected by the Fourth Amendment was invaded" by detaining two packages for twenty-nine hours before a warrant was secured. *Id.* at 253. While the *Van Leeuwen* Court reached its conclusion based on the specific facts before it—which included that the two packages at issue appeared suspicious and were going to separate destinations—I find that Mr. Kamaldoss's case presents similar facts. Each package was of a "suspicious character," *id.*, and all five packages were going to different destinations, *see* Kamaldoss Mot. Ex. A, at Attach. A, ECF No. 159-1. Given these facts, I do not find the length of the delay to weigh in Mr. Kamaldoss's favor. Because, as I have found, factors two and three also weigh strongly against Mr. Kamaldoss, and factor four weighs only slightly in his favor, I conclude that the government's delay in securing a warrant to search Mr. Kamaldoss's packages was not constitutionally unreasonable.

The weight to be accorded to the fifteen-day delay between when Mr. Navaratnarajah's packages were seized and when a warrant was issued is less clear. In *United States v. Martin*, 157 F.3d 46, the Second Circuit held that an eleven-day delay in securing a warrant to search seized packages was acceptable because, *inter alia*, the period included two weekends and a holiday; the owner of the packages had put them in the stream of mail; and the packages' seizure did not restrain the owner's liberty. *See id.* at 54. The *Martin* court noted, however, that "[i]n some circumstances eleven days might well constitute an unreasonable delay." *Id.* Since then, the Second Circuit has

held that a "month-long delay well exceeds what is ordinarily reasonable." *Smith*, 967 F.3d at 207. Fifteen days falls somewhere in between the eleven days affirmed in *Martin* and the month-long delay criticized in *Smith*. Given these precedents, I am inclined to find that here, where the fifteen-day delay included two weekends and involved packages of contraband that were put into the stream of mail, this period of delay should not weigh against the government. Moreover, considering how strongly factors two and three weigh against Mr. Navaratnarajah, this first factor is not dispositive: measuring all four factors together, the scale tips in favor of the government. Accordingly, the delay in securing a warrant to search Mr. Navaratnarajah's packages was not unreasonable, and the contents of his packages, like those of Mr. Kamaldoss's, are admissible.[16]

B. The June 14, 2019, and June 24, 2019, searches of forensic copies of Mr. Kamaldoss's electronic devices.

On May 24, 2019, the government secured a warrant to search the forensic copies of Mr. Kamaldoss's electronic devices. *See* Forensic Search Warrant. Pursuant to this warrant, the forensic copies were reviewed by Special Agent Connor at least twice on June 14, 2019, and once on June 24, 2019. Kamaldoss Mot. 28. Mr. Kamaldoss now moves to suppress these searches on the ground that Agent Connor's affidavit in support of the May warrant included tainted evidence. *Id.* at 27–28. Specifically, Mr. Kamaldoss alleges that paragraphs fifty-one through fifty-three of Agent Connor's affidavit describe information that was unlawfully obtained during the April 23 border search.[17] *Id.* at 27; *see also id.* at 24–26. These paragraphs reference types of information

[16] Because I find that that the government's one- and fifteen-day delays in securing warrants to search Mr. Kamaldoss's and Mr. Navaratnarajah's packages were reasonable, I decline to address the government's alternative argument: that defendants forfeited their Fourth Amendment interests in the packages when they put them in the stream of mail using fictional return addresses and thus do not have standing to challenge the packages' search.

[17] In his suppression motion, Mr. Kamaldoss principally contends that the information referenced in paragraphs fifty-one through fifty-three was based on Special Agent Connor's May review of the forensic copies. *See* Kamaldoss Mot. 27–28. However, in his reply to the government's

that were seen by border agents upon their preliminary review of Mr. Kamaldoss's electronic devices. *See* Forensic Search Warrant Appl. ¶¶ 51−53. Mr. Kamaldoss argues that the May warrant's reliance on this evidence renders the warrant constitutionally infirm and that the June searches should be suppressed as a result. Kamaldoss Mot. 28. Mr. Kamaldoss also seeks suppression on two further grounds: first, because the forensic images were obtained in violation of his Fifth and Fourth Amendment rights; and second, because under the terms of the warrant, Special Agent Connor was required to execute his search by June 7, 2019. *Id.* at 28 n.13; *see also* Forensic Search Warrant 1. I find none of Mr. Kamaldoss's arguments availing.

As an initial matter, Mr. Kamaldoss misapprehends the governing law on "tainted" warrants. "[A]lthough unlawfully obtained evidence should not be included in an affidavit [in support of a warrant], it is well established that the mere inclusion of tainted evidence in an affidavit does not, by itself, taint the warrant or the evidence seized pursuant to the warrant." *United States v. Peeples*, 962 F. 3d 677, 688 (2d Cir. 2020) (internal quotation marks and citation omitted). Instead, "a reviewing court should excise the tainted evidence and determine whether the remaining, untainted evidence would provide a neutral magistrate with probable cause to issue a warrant." *Id.* at 688–89 (internal quotation marks and citation omitted). Here, ample additional evidence was included in Agent Connor's affidavit in support of the May 24 warrant—indeed, only a few paragraphs in his affidavit describe the April 23 search of Mr. Kamaldoss's devices and

---

opposition, Mr. Kamaldoss argues that the warrant was tainted "by the April 2019 border search and/or by subsequent warrantless searches conducted by [Special Agent] Connor [in May]." *See* Kamaldoss Reply 16−17. On my read of Special Agent Connor's application for the May 24 warrant, paragraphs fifty-one through fifty-three describe content observed on Mr. Kamaldoss's electronic devices on April 23 and relayed to Agent Connor by the border agents. *See* Forensic Search Warrant Appl. ¶¶ 52−53 (describing what law enforcement agents observed during a preliminary review of both devices). Because there is no evidence that paragraphs fifty-one through fifty-three were based on Agent Connor's May searches, I consider Mr. Kamaldoss's claim with respect to the April 23 border search only.

the contents thereof. *See generally* Forensic Search Warrant Appl. But in any event, I need not engage in such analysis: as I have already found that the April 23 border search was constitutional, *see supra* Discussion II, there is no tainted evidence to excise. Mr. Kamaldoss's second additional argument—that suppression is proper because the forensic images were initially obtained in violation of his Fifth and Fourth Amendment rights—fails for this same reason.[18]

Regarding Mr. Kamaldoss's final argument—that the June searches should be suppressed because they occurred after the warrant's June 7 execution date—the government is correct that Federal Rule of Criminal Procedure 41(e)(2)(B) resolves this issue. *See* Gov't Opp'n 27 n.4. Under Rule 41(e)(2)(B), the time for executing a warrant for the seizure or copying of electronically stored information "refers to the seizure or on-site copying of the media or information, and *not* to any later off-site copying or review." Fed. R. Crim. P. 41(e)(2)(B) (emphasis added). Accordingly, "[u]nless otherwise specified, the warrant authorizes a later review of the . . . [seized or copied] information consistent with the warrant." *Id.* No such specification was listed on the May 24 warrant, which meant that while Agent Connor had to seize the forensic copies by June 7, he was allowed to review them thereafter. This is exactly what Agent Connor did. *See* Kamaldoss Mot.

[18] Even assuming, *arguendo*, that I had concluded that the April 23 border search was impermissibly broad, suppression would still be improper because Agent Connor conducted his searches in good faith reliance on the May 24 warrant. "If a reviewing court determines that a search warrant was not supported by probable cause, a motion to suppress will still be denied if the court finds that the officers who conducted the search acted in good faith reliance on a facially valid warrant." *United States v. Salameh*, 152 F.3d 88, 114 (2d Cir. 1998). Only in four situations does this exception not apply: "(1) [W]here the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable." *United States v. Clark*, 638 F.3d 89, 100 (2d Cir. 2011) (citation omitted). None of these situations applies here. Most relevant and as just described, the application supporting the warrant contained ample indicia of probable cause separate from the references to the April 23 border search. Agent Connor's reliance on the warrant and subsequent search of the forensic copies were therefore reasonable and in good faith.

Ex. I, at 4 ("Rep't of Investigation") (discussing Agent Connor's review of the forensic copies on June 4, 2019, three days before June 7).

C. Mr. Kamaldoss's Apple and Yahoo email accounts.

On May 1, 2019, the government obtained a warrant to search materials associated with Mr. Kamaldoss's Apple iCloud account. Kamaldoss Mot. 9–10, 31. Just a few weeks later, on May 30, the government obtained search warrants requiring Oath Holdings, the parent company of Yahoo, to produce emails associated with Mr. Kamaldoss's two Yahoo accounts. *Id.* at 10, 31. Mr. Kamaldoss contends that suppression of this material is appropriate because all three search warrants relied upon information that was learned by agents during the April 23 border search. *Id.* at 30−31. For the very same reasons that this argument previously failed, *see supra* Discussion III.B, so too does it fail here.

Propounding another ground for suppression, Mr. Kamaldoss argues that the warrants authorizing the search of his Yahoo email accounts were overbroad and thus violated the Fourth Amendment. Kamaldoss Mot. 32−34. Specifically, both search warrants required Oath Holdings to disclose all emails associated with Mr. Kamaldoss's two Yahoo email accounts without any limiting time period, even though probable cause for the warrant was based on events post-dating May 2018. *See id.* at 32–33; Kamaldoss Mot., Exs. N & O (collectively, "Yahoo Warrants and Applications"), ECF No. 159-1.

"To achieve its goal, the Warrants Clause requires particularity and forbids overbreadth." *United States v. Cioffi*, 668 F. Supp. 2d 385, 390 (E.D.N.Y. 2009). Whether a warrant is overbroad turns on whether the "description of the objects to be seized is broader than can be justified by the probable cause upon which the warrant is based." *United States v. Nejad*, 436 F. Supp. 3d 707, 725 (S.D.N.Y. 2020). Although there is agreement among district courts in this circuit "that a time

frame is relevant [to the question of overbreadth], there is no apparent consensus as to when one is required." *United States v. Cohan*, 628 F. Supp. 2d 355, 366 (E.D.N.Y. 2009) (emphasis omitted) (collecting cases addressing time frame limitations in the context of business-record search warrants). And in the context of electronic information, several courts in this and other circuits have "upheld the [g]overnment's ability to obtain the entire contents of the email account to determine which particular emails come within the search warrant." *United States v. Scully*, 108 F. Supp. 3d 59, 95 (E.D.N.Y. 2015) (collecting cases); *see, e.g.*, *United States v. Bowen*, 689 F. Supp. 2d 675, 682 (S.D.N.Y. 2010) ("Nor does the Fourth Amendment require the executing authorities to delegate a pre-screening function to the internet service provider or to ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searching."), *aff'd sub nom*, *United States v. Ingram*, 490 F. App'x 363 (2d Cir. 2012).

Here, the warrants at issue required Oath Holdings to *disclose* all information in its possession but authorized the government to *seize* only certain types of communications and information dated May 1, 2018, or after. In light of the limitations set on the warrants and existing caselaw on the seizure of email accounts, I am inclined to find that the warrants were not overbroad. This conclusion is not compelled, however because the agents acted in good faith reliance on the warrants' contents. *See Nejad*, 436 F. Supp. 3d at 732; *Levy*, 2013 WL 664712, at *11. "[E]vidence seized pursuant to an overly broad search warrant will be suppressed only if the warrant was so facially invalid that the executing agents could not reasonably have relied on it." *United States v. Wapnick*, No. 92-CR-419 (CBA), 1993 WL 86480, at *7 (E.D.N.Y. Mar. 16, 1993), *aff'd*, 60 F.3d 948 (2d Cir. 1995).[19] Because "the Second Circuit has never spoken to when,

[19] Because Mr. Kamaldoss has challenged the search warrants only on the ground that they failed to include a limiting time period, the other exceptions to the rule that suppression is improper where officers act in good faith reliance on a seemingly valid warrant, *see supra* n.18, are not at

if at all, time-frames are a constitutional requirement . . . [for] search warrants, and district courts in this circuit have not converged upon a clear rule," *Cohan*, 628 F. Supp. 2d at 367, "it cannot be said that [the] executing officers should have realized a lack of date limitation constituted a facial deficiency in the [s]earch [w]arrant such that reliance on it would be unreasonable," *Levy*, 2013 WL 664712, at *11; *see also United States v. Jacobson*, 4 F. Supp. 3d 515, 527 (E.D.N.Y. 2014) ("[T]he fact that the precise relevance of the absence of an express time frame on the particularity and breadth of a warrant has yet to be settled in this [c]ircuit further supports the idea that agents reasonably relied on the magistrate's authorization and should be protected by the 'good faith' exception."); *Nejad*, 436 F. Supp. 3d at 732 (finding that under the good-faith exception, the fruits of a warrant to search emails should not be suppressed because "there is no consensus in this [c]ircuit as to when temporal limitations are required—or when the lack thereof alone may invalidate an otherwise valid search warrant" (internal citation omitted)). Accordingly, even assuming, *arguendo*, that the May 30 warrants were overbroad for lack of a time frame, "the good-faith exception to the exclusionary rule [would] render[] suppression unwarranted." *Cohan*, 628 F. Supp. 2d at 368.[20]

IV. Dismissal of the Underlying and Superseding Indictments Is Improper.

In a final effort to stall his criminal case, Mr. Kamaldoss argues that, regardless of my

---

issue. Accordingly, I decline to address them.

[20] In his suppression motion, Mr. Kamaldoss also contends that the Oath Holdings search warrants were improperly executed because the government seized information predating May 2018, even though the warrant authorized it to seize certain categories of information only if that information was created *after* May 1, 2018. Kamaldoss Mot. 33−34. In support of his argument, Mr. Kamaldoss points to emails produced by the government in discovery that dated back to 2012. *Id.* at 34. The government has since clarified that these emails were produced pursuant to the government's discovery obligations under Federal Rule of Criminal Procedure 16(a)(1)(E)(iii) and will not be reviewed or used by the government at trial except to authenticate the account data. Gov't Opp'n 30−31. I therefore decline to address Mr. Kamaldoss's argument.

rulings on his suppression motions, I should dismiss his underlying and superseding indictments. Kamaldoss Mot. 36. His reason for suggesting such drastic action is curious: because the FDA's authority to conduct criminal investigations derives from the Federal Food, Drug, and Cosmetic Act ("FDCA"), 21 U.S.C. §§ 301−399d, Mr. Kamaldoss posits that the agency does not have jurisdiction to investigate violations of the Controlled Substances Act ("CSA"), 21 U.S.C. § 801 *et seq.*, the Act under which Mr. Kamaldoss is charged. *Id.* In other words, because the FDA's investigation—undertaken with other agencies, including the Department of Homeland Security—led to the discovery of evidence that was used to indict Mr. Kamaldoss under the CSA, the FDA exceeded the scope of its investigative authority and Mr. Kamaldoss's underlying and superseding indictments should be dismissed. This logical leap is without authority. Indeed, in support of his argument, Mr. Kamaldoss cites not a single case concluding that an indictment should be dismissed because the "wrong" federal agency was involved in the defendant's investigation, and I have found no such proposition in the course of my independent research. As the government points out, this could be because "[w]hich particular law enforcement agencies participated in the investigation prior to" the issuance of an indictment by the grand jury "has no conceivable relevance to the indictment['s] validity." Gov't Opp'n 36. After all, the FDA was not responsible for bringing the case before the grand jury or issuing the indictment. Accordingly, I see no meritorious ground for dismissing Mr. Kamaldoss's original and superseding indictments.

CONCLUSION

Because I find that Mr. Kamaldoss's and Mr. Navaratnarajah's constitutional rights were not violated and that there is no basis to dismiss the superseding indictment in this case, their pre-trial motions are denied.

SO ORDERED.

/s/
Allyne R. Ross
United States District Judge

Dated: April 22, 2022
Brooklyn, New York